

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-023331

(43)Date of publication of application : 23.01.1996

(51)Int.Cl.

H04L 9/06

H04L 9/14

G09C 1/00

H04K 1/00

(21)Application number : 06-156307

(71)Applicant : MURATA MACH LTD

(22)Date of filing : 07.07.1994

(72)Inventor : MURAKAMI YASUMICHI  
ITO KAZUHITO

## (54) METHOD AND DEVICE FOR CIPHERING COMMUNICATION

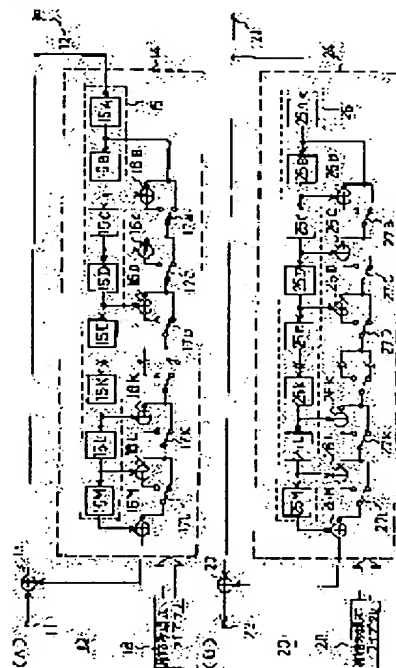
### (57)Abstract:

**PURPOSE:** To attain ciphering and deciphering with simple configuration by applying self synchronization ciphering to communication information based on a selected irreducible polynomial, sending the to the received information.

**CONSTITUTION:** A bit string received by a shift register 15 is subject to arithmetic operation at prescribed bits while being shifted sequentially therein and the result is given to an adder 13. The shifting operation is conducted synchronously with an input operation of the bit string to a terminal 11. That is, the ciphering is conducted by dividing a message polynomial representing the received bit string with coefficients in descending order by a ciphering generating polynomial (key). Then the bit string received from an input terminal 21 is given to an adder 23 and a primitive polynomial configuration section 24.

The adder 23 receives the bit string from the terminal 21 and the primitive polynomial configuration section 24. An output of the adder 23 is outputted from a terminal 22

as a decoded bit string. That is, a decoding circuit 20 uses the same primitive polynomial as that of a ciphering circuit 10 to decode the ciphered data.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-23331

(43) 公開日 平成8年(1996) 1月23日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L	9/06			
	9/14			
G 0 9 C	1/00	7259-5 J		
H 0 4 K	1/00	Z		

H 0 4 L 9/ 02 Z  
審査請求 有 請求項の数 6 O L (全 13 頁)

(21) 出願番号 特願平6-156307

(22) 出願日 平成6年(1994) 7月7日

(71) 出願人 000006297

村田機械株式会社

京都府京都市南区吉祥院南落合町3番地

(72) 発明者 村上 恭道

京都市伏見区竹田向代町136番地 村田機械株式会社本社工場内

(72) 発明者 伊藤 一仁

京都市伏見区竹田向代町136番地 村田機械株式会社本社工場内

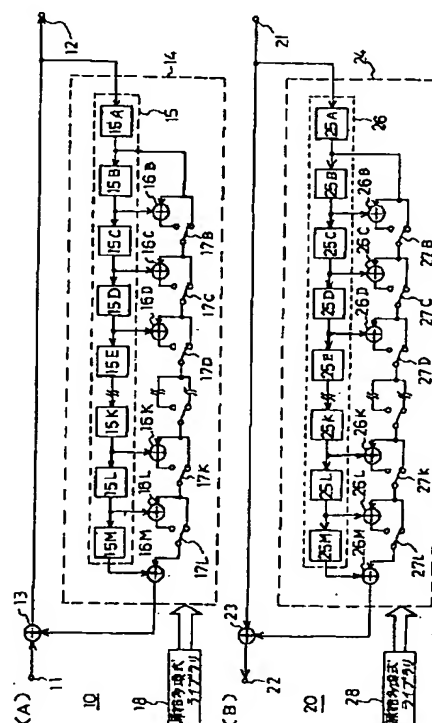
(54) 【発明の名称】 暗号化通信方法及び装置

(57) 【要約】

【目的】 伝送路上で通信データに欠落を生じ易い通信回線でも、暗号化、復号化が可能な暗号化通信装置及び方法を提供する。

【構成】 複数の既約多項式をもつ自己同期形の暗号化／復号化回路を使用する。暗号化通信に先立ち、送受間で暗号化に使用する既約多項式を選択する。送信側では、選択された既約多項式によって通信情報を暗号化して送信する。受信側では、選択された既約多項式によって受信した通信情報を復号化する。

【効果】 既約多項式そのものを鍵とすることによって、簡易な構成で、欠落データの影響を排除できる。



## 【特許請求の範囲】

【請求項 1】 送信局及び受信局に複数の既約多項式を備え、暗号化通信に使用する少なくとも 1 つの既約多項式を送信局及び受信局で選択し、送信局は選択された既約多項式によって通信情報を自己同期暗号化して送信し、受信局は選択された既約多項式によって受信した通信情報を自己同期復号化することを特徴とする暗号化通信方法。

【請求項 2】 請求項 1 に記載の暗号化通信方法において、前記既約多項式は原始多項式であることを特徴とする暗号化通信方法。

【請求項 3】 複数の既約多項式を記憶した記憶手段と、前記記憶手段に記憶された既約多項式から少なくとも 1 つの既約多項式を選択する選択手段と、前記選択手段に基づき任意の既約多項式を構成する少なくとも 1 つの既約多項式構成手段と、前記既約多項式構成手段によって構成された既約多項式によって暗号化、復号化を行う自己同期暗号化／復号化手段を備えることを特徴とする暗号化通信装置。

【請求項 4】 請求項 3 に記載の暗号化通信装置において、前記選択手段は乱数発生手段を含むことを特徴とする暗号化通信装置。

【請求項 5】 請求項 3 に記載の暗号化通信装置において、前記選択手段は通信相手局から受信した情報に基づいて既約多項式を選択することを特徴とする暗号化通信装置。

【請求項 6】 請求項 3 乃至 5 の各々に記載の暗号化通信装置において、前記既約多項式は原始多項式であることを特徴とする暗号化通信装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】この発明は、デジタルデータ通信に適する暗号化通信方法及び装置に関する。さらに詳しくは、伝送路上で通信データに欠落が生じてでも使用することが可能な暗号化通信方法及び装置に関する。

## 【0002】

【従来の技術】デジタルデータ通信における通信の傍受から通信の秘密を守るために、通信情報を暗号化することが行われている。図 8 (A) にその一例を示す。端子 4 1 から暗号化前のビット列（平文情報）が入力され、端子 4 2 から暗号化されたビット列（暗号情報）が出力される。4 5 は 13 ビットのシフトレジスタであり、暗号化の鍵（キー）となるビット列が予め格納されている。端子 4 1 から加算器 4 3 へ 1 ビットのデータが入力される毎に、シフトレジスタ 4 5 のビット列は矢印 4 9 の方向へ 1 ビットづつシフトされ、1 ビットのデータが加算器 4 3 へ入力される。

【0003】加算器 4 3 は、端子 4 1 とシフトレジスタ 4 5 から入力されたデータを演算（排他的論理和）し、演算結果を暗号情報として端子 4 2 から出力する。シフ

トレジスタ 4 5 の最上位ビット 4 5 M のデータは、加算器 4 3 へ入力されると共に、シフトレジスタ 4 5 の所定位置にある加算器 4 6 と、最下位ビット 4 5 A にも入力される。シフトレジスタ 4 5 の内容は  $(2^{12} - 1)$  回のシフトを繰り返す毎に同じ内容となる。

【0004】復号化（読取）する場合には、図 7 (B) に示すように、暗号化とは逆の手順をとる。端子 5 1 から入力された暗号化ビット列と、シフトレジスタ 5 5 のビット列は、加算器 5 3 へ入力される。加算器 5 3 の演算結果が復号されたビット列として端子 5 2 から出力される。シフトレジスタ 5 5 には、シフトレジスタ 4 5 と同じビット列（鍵）が予め格納されており、シフトする毎に、シフトレジスタ 5 5 の最上位ビット 5 5 M のデータは、加算器 5 3 へ入力されると共に、シフトレジスタ 5 5 の所定位置にある加算器 5 6 と、最下位ビット 5 5 A にも入力される。

## 【0005】

【発明が解決しようする課題】しかしながら、上述の方法では、復号の時、伝送路上でビット列に欠落が生じて、シフトレジスタ 5 6 のビット列は、欠落後のビット列に同期してシフトされることになる。欠落の発生以降の暗号化ビット列と、復号化する鍵（シフトレジスタ 5 6 のビット列）にズレが生じることになり、復号することができない。もし、伝送路上でビット列に欠落が生じると、その後の暗号化ビット列を復号できなくなる。

【0006】デジタルデータ通信には様々な通信手順があり、これらのなかには伝送路上での伝送誤りの訂正や、欠落データの検出・再送を行う誤り訂正機能を備えているものもある。伝送路上での欠落データを回復できる誤り訂正機能を備えた通信手順においては、上述のような暗号化方法を採用することができるが、再送の為に多くの伝送時間を必要としたり、より高度な暗号化、復号化処理を必要とする。本発明の目的は、伝送路上で欠落データが生じて、欠落データの再送が不要であり、簡易な構成で暗号化、復号化が可能な暗号化通信方法及び装置を提供することである。

## 【0007】

【課題を解決するための手段】本発明の暗号化通信方法では、送信局及び受信局に複数の既約多項式を備え、暗号化通信に使用する少なくとも 1 つの既約多項式を送信局及び受信局で選択し、送信局は選択された既約多項式によって通信情報を自己同期暗号化して送信し、受信局は選択された既約多項式によって受信した通信情報を自己同期復号化することを特徴としている。

【0008】また、本発明の暗号化通信装置では、複数の既約多項式を記憶した記憶手段と、前記記憶手段に記憶された既約多項式から少なくとも 1 つの既約多項式を選択する選択手段と、前記選択手段に基づき任意の既約多項式を構成する少なくとも 1 つの既約多項式構成手段と、前記既約多項式構成手段によって構成された既約多

項式によって暗号化、復号化を行う自己同期暗号化／復号化手段を備えることを特徴としている。

【0009】

【作用】複数の既約多項式を備える自己同期形暗号化／復号化手段をそれぞれ送信機／受信機に備える。暗号化すべきビット列の通信に先立ち、送受間で複数の既約多項式の内から暗号化に使用する少なくとも1つの既約多項式（以下、特定生成多項式と呼ぶ）を選択し、暗号化／復号化手段に特定生成多項式（鍵）を構成する。

【0010】特定生成多項式が構成された後、送信側は特定生成多項式を使用して送信ビット列を暗号化する。受信側は、特定生成多項式を使用して受信ビット列を復号化する。自己同期型暗号化／復号化手段を使用しているの、伝送路上においてデータの欠落が発生しても、所定ビット後には、欠落データによる影響を排除できる。また、既約多項式に原始多項式を使用することにより、ランダム度が最大のビットシーケンスを得ることができ、効率的な暗号化ができる。

【0011】

【実施例】図1（A）は、本発明による暗号化回路10を示した図である。11は入力端子であり、平文のビット列が入力される。12は出力端子であり、暗号化されたビット列が出力される。14は原始多項式構成部、1\*

\* 3は演算（排他的論理和）を行う加算器であり、加算器13には、端子11と原始多項式構成部14からビット列が入力される。加算器13の出力は暗号化されたビット列として端子12から出力されると共に、原始多項式構成部14にも入力される。

【0012】次に、原始多項式構成部14について説明する。原始多項式構成部14は、15A～Mより成る13ビットのシフトレジスタ15、12個の加算器16B～M、加算器16B～Lに設けられたスイッチ17B～Lを備えている。スイッチ17B～Lは、加算器16B～Lを有効化又は無効化するためのものである。

【0013】本実施例では、12次の生成多項式を使用し、既約多項式に原始多項式を使用している。12次の生成多項式は、表1に示すように、144個の原始多項式を持っている。原始多項式ライブラリ18は、表1に示された原始多項式番号とこれに対応する原始多項式データを記憶している。原始多項式データの1又は0は各項の有無を示し、（L～B）は対応するスイッチ17を示す。原始多項式構成部14は、原始多項式ライブラリ18に基づいて、144個の原始多項式から任意の原始多項式を構成できる。

【0014】

【表1】

原始多項式ライブラリ													
原始多項式 番号	原始多項式データ												
	$X^{12}+X^{11}+X^{10}+X^9$	$+X^8$	$+X^7$	$+X^6$	$+X^5$	$+X^4$	$+X^3$	$+X^2$	$+X^1$	$+1$			
	(L	K	J	I	H	G	F	E	D	C	B)		
1	1	0	0	0	0	0	1	0	1	0	0	1	1
2	1	0	0	0	0	0	1	1	0	1	0	0	1
3	1	0	0	0	0	0	1	1	1	1	0	1	1
4	1	0	0	0	0	0	1	1	1	1	1	0	1
5	1	0	0	0	0	1	0	0	1	1	0	0	1
.							.						
.							.						
..							(一部省略)						
.							.						
...							.						
142	1	1	1	1	1	1	0	1	1	1	0	1	1
143	1	1	1	1	1	1	0	1	1	1	1	0	1
144	1	1	1	1	1	1	1	0	0	1	0	0	1

【0015】例えば、表1にある原始多項式番号1の原始多項式

$$X^{12} + X^6 + X^4 + X + 1$$

を構成する場合には、スイッチ17B～Lのうち、スイッチ17B、E、Gを加算器16B、E、G側に接続して、加算器16B、E、Gを有効状態にする。このよう

に、原始多項式データが1になっている項に対応するスイッチ17B～Lを加算器16B～Lに接続することによって、任意の原始多項式を構成することができる。

【0016】加算器13から出力されたビット列は、端子12から出力されると共に、シフトレジスタ15の最下位ビット15Aにも入力される。シフトレジスタ15

へ入力されたビット列は、順次シフトしながら、所定ビットでは演算を行い、加算器 13 へ入力される。このシフト動作は、端子 11 へのビット列の入力動作と同期して行われる。つまり、入力ビット列を降べきの順の係数で表したメッセージ多項式を、暗号化生成多項式（鍵）で除算することによって、暗号化が行われる。

【0017】次に、図 1 (B) を参照し、暗号文を復号する復号化回路 20 について説明する。21 は入力端子であり、暗号化されたビット列が入力される。22 は出力端子であり、復号化されたビット列が出力される。24 は原始多項式構成部、23 は演算（排他的論理和）を行う加算器である。

【0018】入力端子 21 から入力されたビット列は、加算器 23 と原始多項式構成部 24 へ入力される。加算器 23 には、端子 21 と原始多項式構成部 24 からビット列が入力される。加算器 23 の出力は復号化されたビット列として端子 22 から出力される。

【0019】原始多項式構成部 24 は、原始多項式構成部 14 と同様に、25 A ~ M より成るシフトレジスタ 25、加算器 26 B ~ M、スイッチ 27 B ~ L から構成されている。復号化回路 20 は、暗号化回路 10 と同様に、表 1 に示された原始多項式番号と、原始多項式データを記憶した原始多項式ライブラリ 28 を備え、任意の原始多項式を構成することができる。

【0020】原始多項式構成部 24 では、端子 21 からのビット列の入力と同期して、シフトレジスタ 25 のシフトを行い、加算器 26 B ~ M、スイッチ 27 B ~ L で定義された演算を行う。原始多項式構成部 24 から出力されたビット列は、加算器 23 へ入力される。

【0021】復号化回路 20 で、暗号化回路 10 と同じ原始多項式を使用することにより、暗号化回路 10 によって暗号化された暗号文を復号化することができる。複数の原始多項式から、いずれの原始多項式を使用するかは、通信すべきビット列の送信に先立ち、乱数や演算等を利用して、送受信間で取り決めればよい。

【0022】暗号化回路 10、復号化回路 20 では、12 次の原始多項式を使用したもので、伝送路上でデータ欠落が生じて 12 ビット後には、データ欠落の影響を排除することができる。次数は 12 次より多くても、小さくてもよい。一般的には、次数が大きくなるほど、暗号化の鍵が増えることになる。例えば、13 次の原始多項式は 630 個あり、次数を 1 次大きくするだけで、原始多項式（鍵）の数を飛躍的に増加させることができる。

【0023】原始多項式はランダム度が最も高く、最も効率的な暗号化を行うことができるが、原始多項式以外の既約多項式も鍵として使用することができる。原始多項式以外の既約多項式を使用すると、多項式の次数を上げることなく、鍵の数を大幅に増加させることができる。また、本実施例では、ハードウェアとしてのレジスタ、加算器、スイッチを用いたが、マイクロコンピュー

タとソフトウェア（プログラム）によって本発明を構成することも可能である。

【0024】複数の原始多項式構成部を並列に構成した暗号化回路 30 について、図 2 を参照しながら説明する。暗号化回路 10 に対応する箇所には同じ符号を付している。38 は第 2 原始多項式ライブラリであり、原始多項式ライブラリ 18 と同様に原始多項式番号と原始多項式データを含んでいる。34 は第 2 原始多項式構成部であり、原始多項式構成部 14 と同様にレジスタ 35、加算器 36 B ~ H、スイッチ 37 B ~ G を含み、第 2 原始多項式ライブラリ 38 の原始多項式データに基づき、任意の原始多項式を構成することが可能である。

【0025】原始多項式構成部 14 の加算器 26 M の出力と、第 2 原始多項式構成部 34 のスイッチ 37 G の出力は加算器 36 H 1 へ入力される。加算器 36 H 1 の出力とレジスタ 35 の最上位ビット 35 H の出力は加算器 36 H 2 へ入力される。加算器 36 H 2 の出力と入力端子 11 からの入力ビット列は、加算器 13 へ入力される。加算器 13 の出力が暗号化されたビット列として、出力端子 12 から出力されると共に、多項式構成回路 14 と、第 2 多項式構成回路 34 にも入力される。

【0026】第 2 原始多項式構成部 34 の次数は 7 次であるが、原始多項式構成部 14 の次数と異なれば大きくても、小さくてもよい。いま、暗号化に使用する 2 つの原始多項式の次数をそれぞれ  $m$ 、 $n$  とすると、 $m$ 、 $n$  は  $(2^m - 1)$  と  $(2^n - 1)$  が互いに素であるように設定するのが望ましい。

【0027】暗号化回路 30 のように、次数の異なる複数の多項式構成部を並列に構成することにより、各々の原始多項式の次数は低くても、実質的には大きな次数の原始多項式を使用した場合と同じ効果を得ることができる。また、複数の多項式の内の最大次数ビット後に、欠落データの影響を排除することができる。例えば、暗号化回路 30 のように 12 次と 7 次の原始多項式を使用している場合には、欠落データの発生後、12 ビット後に欠落データの影響を排除することができる。つまり、欠落データの影響を排除するために必要なビット数を増加させることなく、暗号化の鍵を増やすことができる。

【0028】暗号化回路 30 で暗号化された暗号文を復号するには、暗号化回路 30 と同様に、復号化回路 20 に複数の原始多項式構成部を構成すればよく、詳細な説明は省略する。

【0029】次に、上述の暗号化回路 10、復号化回路 20 を用いたデジタル無線電話機 80 について、図 3 を参照しながら説明する。61 はマイクロホンであり、アナログ音声信号を A/D コンバータ 62 へ出力する。A/D コンバータ 62 は、アナログ音声信号を、デジタル音声データへ変換し、音声圧縮符号化回路 63 へ出力する。音声圧縮符号化回路 63 は、デジタル音声データのデータ量を圧縮し、暗号化回路 10 へ出力する。

【0030】暗号化回路10は、原始多項式に基づいて、圧縮されたデジタル音声データを暗号化して、D/Aコンバータ64へ出力する。また、制御部81からの制御データも、D/Aコンバータ64へ出力される。制御部81は、通信相手局との通信回線（周波数）の割り当て、接続、開放等を行うための制御データの解析、生成を行う。また、制御部81は、複数の原始多項式から任意の原始多項式（特定多項式）を選ぶための乱数発生部82を備えている。

【0031】D/Aコンバータ64は、デジタルデータを高周波変調できるように、アナログ信号に変換し、高周波送信部65へ出力する。高周波送信部65は、アナログ信号を変調してアンテナ87から高周波を出力する。86は、送受信でアンテナを共用するためのデュプレクサである。83は操作部、84は表示部、85はブザーである。

【0032】高周波受信部75は、アンテナ87で受信した高周波信号を復調し、A/Dコンバータ74へ出力する。A/Dコンバータ74は、復調されたアナログ信号をデジタル化して、等化处理等を行い、ビット列として、復号化回路20へ出力する。また、ビット列の一部は制御部81へ出力される。復号化回路20は、原始多項式に基づいて、暗号を復号化し、音声圧縮復号化回路73へ出力する。

【0033】音声圧縮復号化回路73は、圧縮符号化されたデジタル音声データを復号化することによって、デジタル音声データを復元し、D/Aコンバータ72へ出力する。D/Aコンバータ72は、デジタル音声データをアナログ音声信号へ変換して、スピーカ71から出力する。

【0034】通信時の手順について、図4を参照しながら説明する。通信相手局は、本実施例のデジタル無線電話機80と同等のものであってもよいし、複数のデジタル無線電話機を一元的に管理する移動通信システムにおける基地局であってもよい。まず、使用者によってデジタル無線電話機80の操作部83で所定の操作が行われると、相手局の呼び出し、通話回線の設定を行う（S1）。

【0035】次に、乱数発生部82で乱数を発生させ、乱数に基づいて、暗号化に使用する原始多項式を示す原始多項式番号を選択する。原始多項式番号は、制御データの一部として、通話相手局へも送信される。暗号化回路10は、選択された原始多項式番号に基づき、原始多項式ライブラリ18から、原始多項式データを取り出し、スイッチ17B～Lを操作して原始多項式を構成する（S2）。原始多項式を選択するために、乱数以外の方法を用いることも可能である。

【0036】原始多項式の構成が完了すると、通話を開始することができる（S3）。マイクロホン61から入力されたアナログ音声信号は、デジタル化、圧縮符号

化、そして、暗号化された後、通話相手局へ送信される。通話が終了すれば、通信回線を開放し、通信を終了する（S4）。

【0037】本実施例と同じ構成のデジタル無線電話機80が、被呼側になった場合について説明する。制御部81が、自局の呼び出しを検出すると、ブザー85を鳴動させる。ブザーに気付いた利用者が操作部83の所定のキー（不図示）を操作すると、デジタル無線電話機80は、着信への応答を行い、通話回線の設定を行う（S1）。

【0038】その後、暗号化に使用する原始多項式を示す原始多項式番号を受信すると、復号化回路20は、原始多項式ライブラリ28から、原始多項式データを取り出し、スイッチ27B～Lを操作して、原始多項式を構成する（S2）。通話が開始されると、高周波受信部75で受信され、A/D変換されたデジタル音声データは、復号化回路20で復号された後、圧縮復号化、アナログ化されてスピーカ71から出力される（S3）。通話が終了すれば、通信回線を開放し、通信を終了する（S4）。

【0039】上述のデジタル無線電話機80では、暗号化に使用する原始多項式を選択するために、発呼側で乱数によって原始多項式番号を選択し、被呼側へ原始多項式番号を送信している。原始多項式を選択は、次のように行うことも可能である。

(1) 被呼側のデジタル無線電話機で乱数によって原始多項式番号を選択し、発呼側へ送信すること。

【0040】(2) 回線接続時に、発呼側、被呼側の電話番号を互いに交換し、いずれか、もしくは、両方に含まれている電話番号と、所定の演算式を使用して原始多項式を選択し、原始多項式を構成し、暗号化通信を行う。演算式が秘密にされていれば、2重の暗号化ができる。

(3) 符号化回路30を使用した場合には、複数の原始多項式を選択する必要があるが、上述の方法を組み合わせで使用することもできる。

【0041】次に、前述の暗号化回路10、復号化回路20を用いたファクシミリ装置100について、図5を参照しながら説明する。読取部101は、文字や図形等の画像をCCD等の光電変換素子、バイナリコンバータ等を用いて、デジタル画像データに変換し、冗長度圧縮符号化回路102へ出力する。冗長度圧縮符号化回路102は、デジタル画像データをMH方式、MR方式等により冗長度圧縮符号化し、暗号化回路10へ出力する。

【0042】暗号化回路10は、冗長度圧縮符号化された画像データを暗号化して、モデム103へ出力する。モデム103はデジタルデータを、電話回線Lで送信できるように変調したり、電話回線Lから受信したアナログ信号を復調する他、通信手順信号の生成、検出を行う。回線制御装置（NCU）104は、電話回線Lとモデム103又は付属電話機105との接続、開放を行

う。

【0043】電話回線Lを通じて通信相手ファクシミリ装置から受信したアナログ信号は、モデム103でデジタルデータに復調され、復号化回路20へ入力される。復号化回路20は、暗号化されたデジタルデータを復号して、冗長度圧縮復号化回路106へ出力する。冗長度圧縮復号化回路106は、暗号を復号されたデジタルデータを冗長度圧縮復号化し、記録部107へ出力する。記録部107は、電子写真記録方式等によってデジタル画像データを記録紙に印字出力する。

【0044】108はファクシミリ装置100を操作するためのキー（不図示）等を備えた操作部、109はファクシミリ装置100の動作状態を表示するための表示部、110は暗号化に使用する原始多項式を選択するための乱数を発生する乱数発生部である。111はファクシミリ装置100の上述の各部を制御する制御部である。

【0045】上述のファクシミリ装置100を被呼側に使用した場合の動作について、図6を参照して説明する。制御部111が、局交換器からの呼び出し信号（C1）を検出すると（S11）、制御部111はNCU104を制御して、電話回線Lとモデム103を接続する（S12）。その後、所定期間内にCNG信号を検出できなければ（S13）、付属電話機105を呼び出し、通話に入るが（S14）、所定期間内にCNGを検出すると、CED信号を送出する（S15）。

【0046】暗号化に使用する原始多項式を示す原始多項式番号となる乱数を乱数発生部110で発生し（S16）、非標準手順を示すNSF信号と共に、本発明の暗号化通信を行う情報と原始多項式番号を送信する（S17）。さらに、CSI信号、DIS信号を送信（S18）した後、NSS信号の検出を行う（S19）。NSS信号を検出することができなければ、発呼局は本発明の暗号化通信が可能でないで、標準手順を実行する（S20）。NSS信号を検出できれば、発呼局は本発明の暗号化通信が可能なので、TSI信号、DCS信号を送信（S21）した後、原始多項式番号に基づいて、復号化回路20の原始多項式構成部24に原始多項式を構成する（S22）。

【0047】モデム103のトレーニング（S23）が終了後、CFR信号を送信し（S24）、FAXメッセージを受信する（S25）。受信されたFAXメッセージは復号化回路20で復号された後、冗長度圧縮復号化回路106でイメージデータに復号され、記録部107で記録紙へ記録される。通信データの終了を示すEOP信号を検出すると（S26）、MCF信号を送信する（S27）。その後、DCN信号を受信すると（S28）、NCU104を制御して、電話回線Lを開放する（S29）。

【0048】次に、上述のファクシミリ装置100を発

呼側に使用した場合の動作について、図7を参照して説明する。ファクシミリ装置100の使用者が、読取部101に原稿を載置した後、操作部108から電話番号を入力し、通信キー（不図示）を操作すると、制御部111は、NCU104を制御して電話回線Lとモデム103を接続して、DTMF信号又はダイヤルパルスを送出する（S31）。その後、制御部111は、CNG信号を送信しながらCED信号の検出を行う（S32、S33）。

10 【0049】CED信号を検出すると、CNG信号の送出を停止し、NSF信号の検出を行う（S34）。NSF信号が検出されない（標準手順の場合）か、もしくは、検出されても本発明の暗号化通信を示すものでない場合には標準手順を行う（S35）。NSF信号が検出されるとCSI信号、DIS信号を受信する（S36）。NSF信号に本発明の暗号化通信を示す情報が含まれている場合には、さらに、暗号化に使用する原始多項式を示す原始多項式番号を検出し、暗号化回路10に原始多項式を構成する（S37）。

20 【0050】さらに、本発明の暗号化通信が可能であることを示す情報を含んだNSS信号、TSI信号、DCS信号を送信する（S38）。モデム103のトレーニングを行い（S39）、CFR信号を受信すると（S40）、FAXメッセージの送信を行う（S41）。読取部101は、載置された原稿を、順次、走査し、デジタルイメージデータに変換して、冗長度圧縮符号化回路102へ出力する。冗長度圧縮符号化回路102は、MH方式等により圧縮符号化して暗号化回路10へ出力する。

30 【0051】暗号化回路10は、原始多項式構成部14で構成された原始多項式により、暗号化を行った後、FAXメッセージをモデム103へ出力する。モデム103は、FAXメッセージを変調して、電話回線Lへ送出する。原稿の送信が完了すると（S42）、EOP信号を送信する（S43）。MCF信号を受信すると（S44）、DCN信号を送信し（S45）、NCU104を制御して電話回線Lを開放する（S46）。

【0052】上述のファクシミリ装置100では、暗号化に使用する原始多項式を選択するために、被呼側で乱数によって原始多項式番号を選択し、発呼側へ原始多項式番号を送信している。原始多項式の選択は、次のように行うことも可能である。

(1) 発呼側ファクシミリ装置で乱数によって原始多項式番号を選択し、被呼側へ送信すること。

【0053】(2) ファクシミリ装置100は付属電話機105を備えているので、使用者が付属電話機105で相手側ファクシミリ装置の使用者と通話を行い、暗号化に使用する原始多項式の番号を選択し、各々の操作部108から原始多項式番号を入力する。発呼側、被呼側の各々のファクシミリ装置100は、操作部108で選択



された原始多項式番号に基づいて原始多項式を構成し、暗号化通信を行う。

【0054】(3) ファクシミリ手順信号である C S I 信号、T S I 信号は、それぞれ被呼側、発呼側ファクシミリ装置の電話番号を含んでいる。発呼側、被呼側の各々のファクシミリ装置 100 は、C S I 信号、T S I 信号のいずれか、もしくは、両方に含まれている電話番号と、所定の演算式を使用して原始多項式番号を選択し、原始多項式を構成し、暗号化通信を行う。演算式が秘密にされていれば、2 重の暗号化ができる。

(3) 符号化回路 30 を使用した場合には、複数の原始多項式を選択する必要があるが、上述の方法を組み合わせで使用することもできる。

#### 【発明の効果】

【0055】本実施例では、通話を行うデジタル無線電話機と画像通信を行うファクシミリ装置について説明したが、発明は伝送路の種類に関係なく適用することができる。また、音声データや画像データに限ることなく、他のデジタルデータ通信にも適用することができる。

【0056】このように、既約多項式そのものを暗号化／復号化の鍵としているので、通信の最初に暗号化に使用する既約多項式を示す情報を 2 局間で選択するだけで、暗号化の鍵を設定することができる。また、自己同期式暗号化／復号化手段を使用しているので、伝送路上でビット列に欠落が生じて、所定ビット後には欠落の影響を排除することができる。

#### 【図面の簡単な説明】

【図 1】本発明の暗号化通信装置の要部を示す図である。

\*

\*【図 2】本発明の暗号化通信装置の要部を示す図である。

【図 3】本発明の暗号化通信装置を示すブロック図である。

【図 4】本発明の暗号化通信方法を示すフローチャートである。

【図 5】本発明の暗号化通信装置を示すブロック図である。

【図 6】本発明の暗号化通信方法を示すフローチャートである。

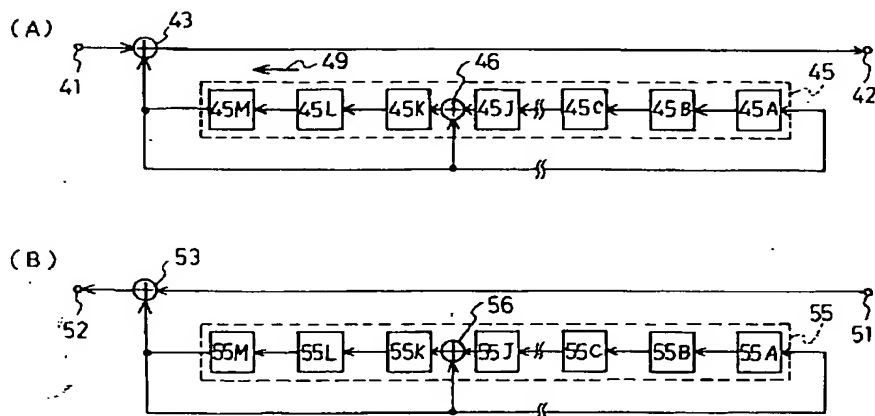
【図 7】本発明の暗号化通信方法を示すフローチャートである。

【図 8】従来の暗号化回路、復号化回路である。

#### 【符号の説明】

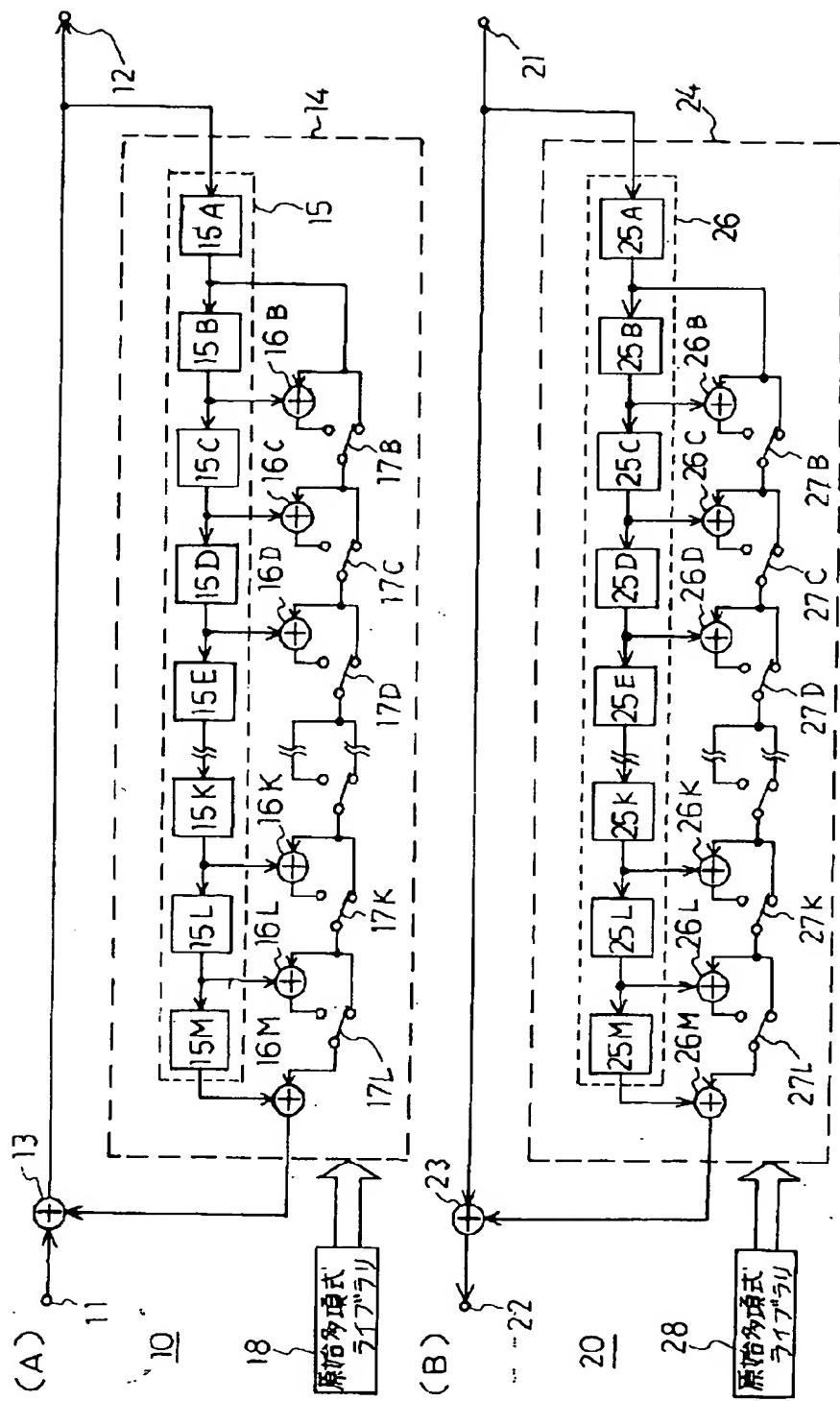
10, 30	暗号化回路
20	復号化回路
11, 21	入力端子
12, 22	出力端子
13, 23	加算器
14, 24, 34	原始多項式構成部
15, 25, 35	シフトレジスタ
16B~M	加算器
26B~M	加算器
36B~H	加算器
17B~L	スイッチ
27B~L	スイッチ
37B~G	スイッチ
18, 28, 38	原始多項式ライブラリ

【図 8】

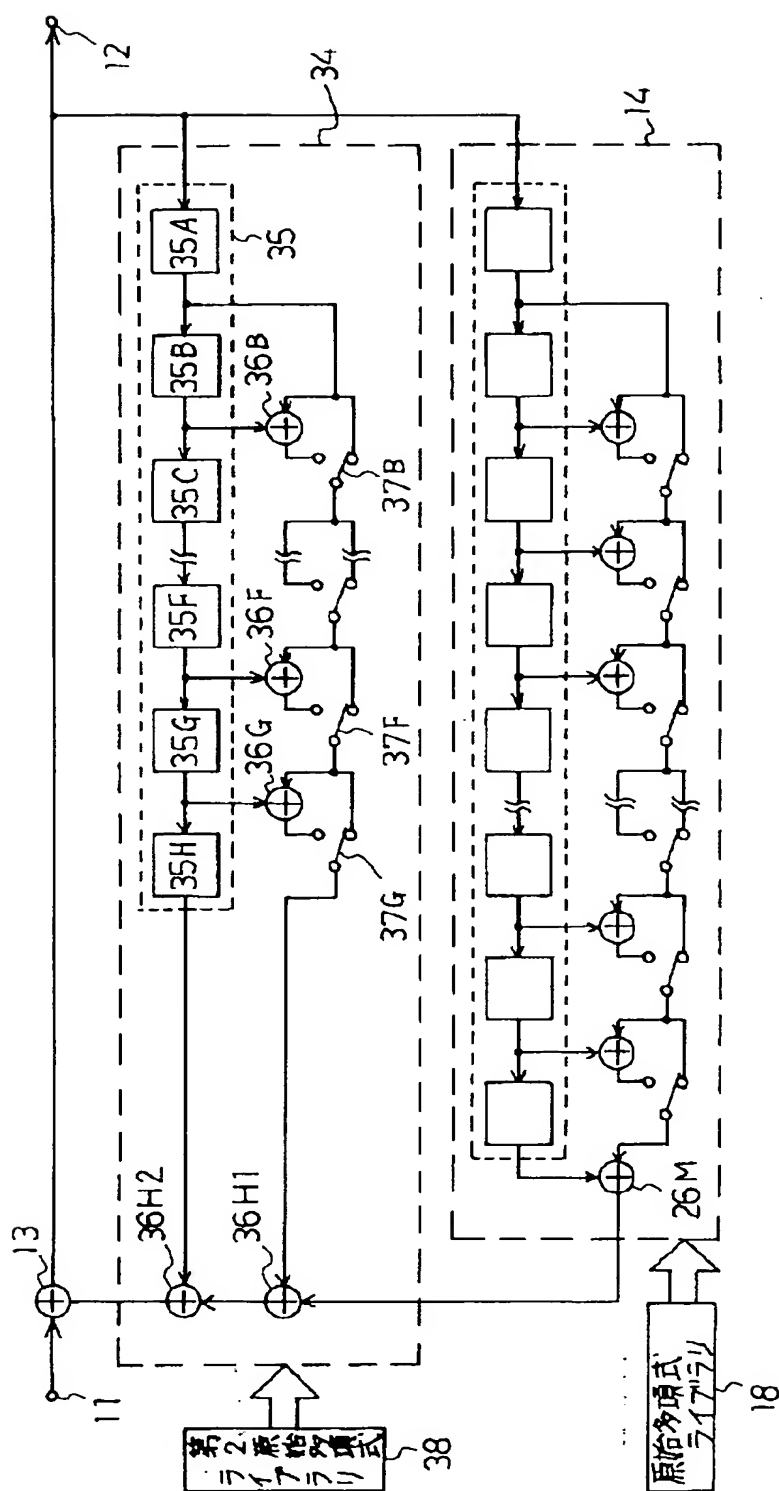




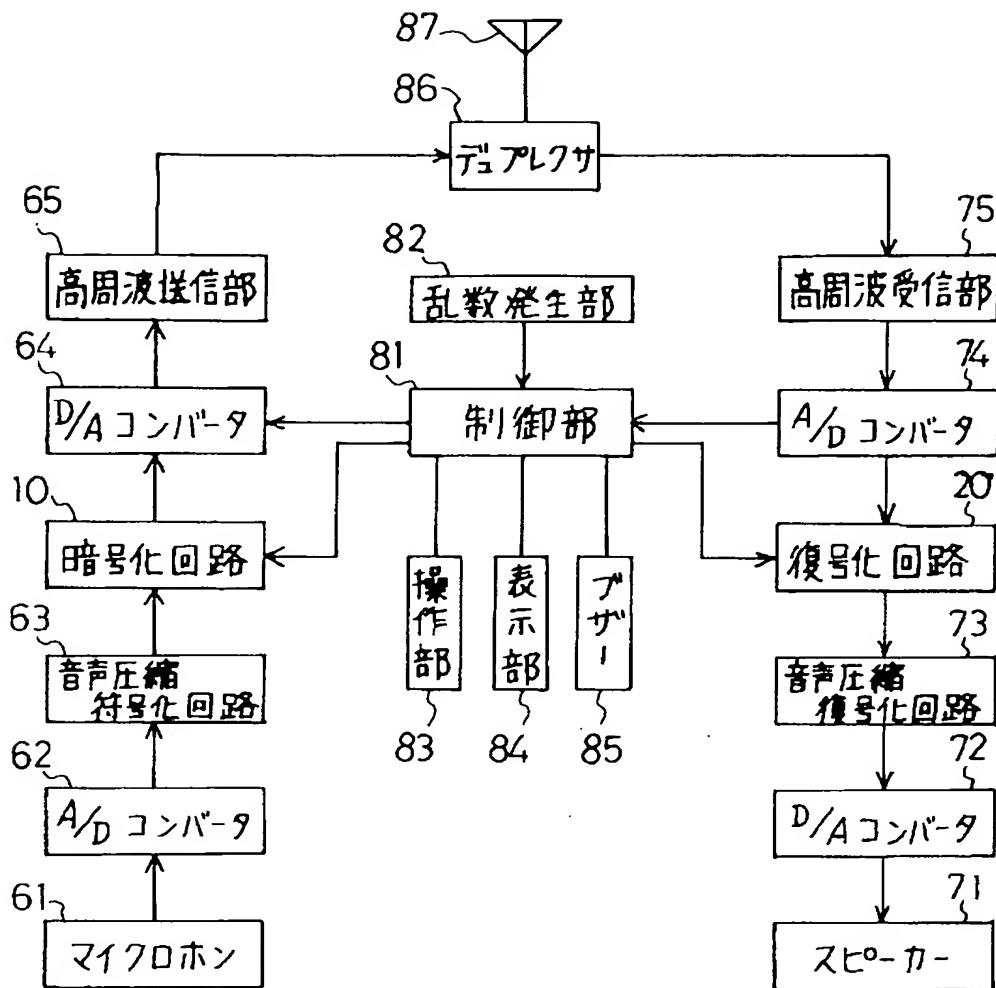
【図 1】



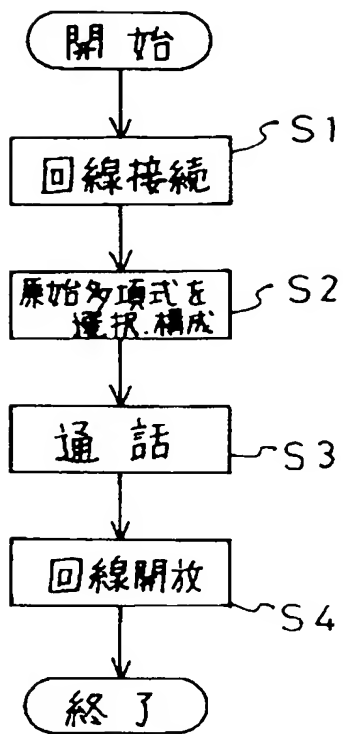
【図 2】



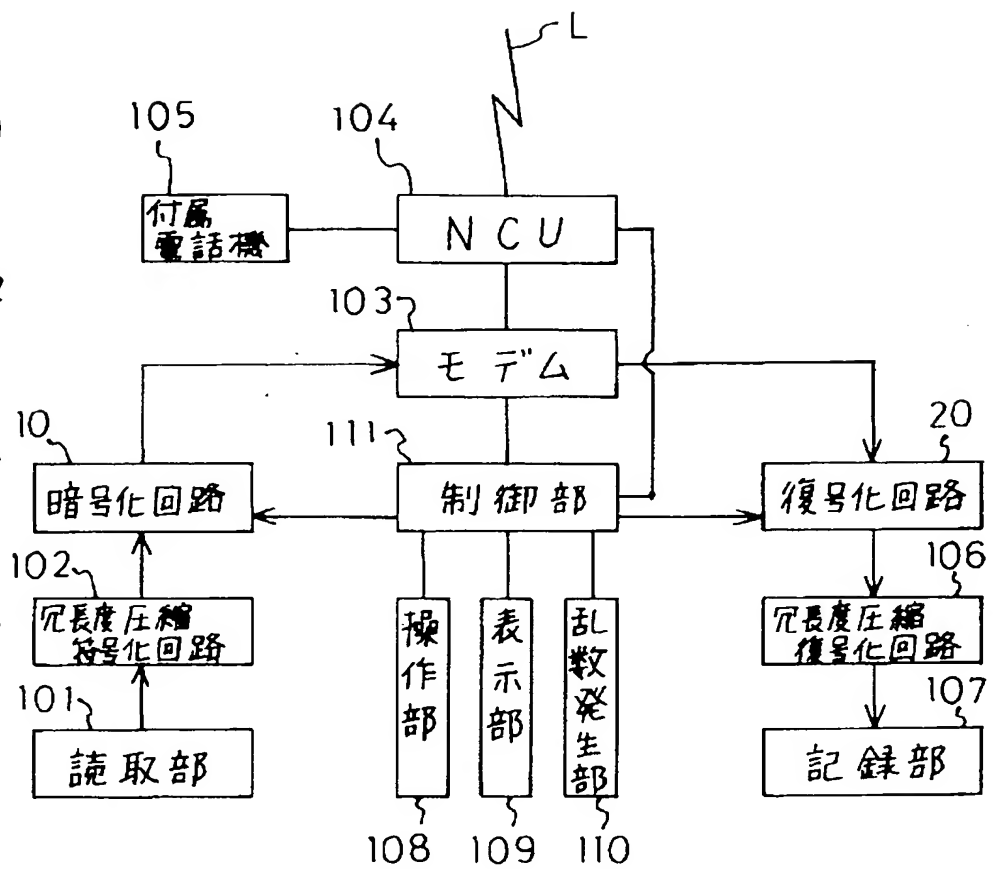
【図3】



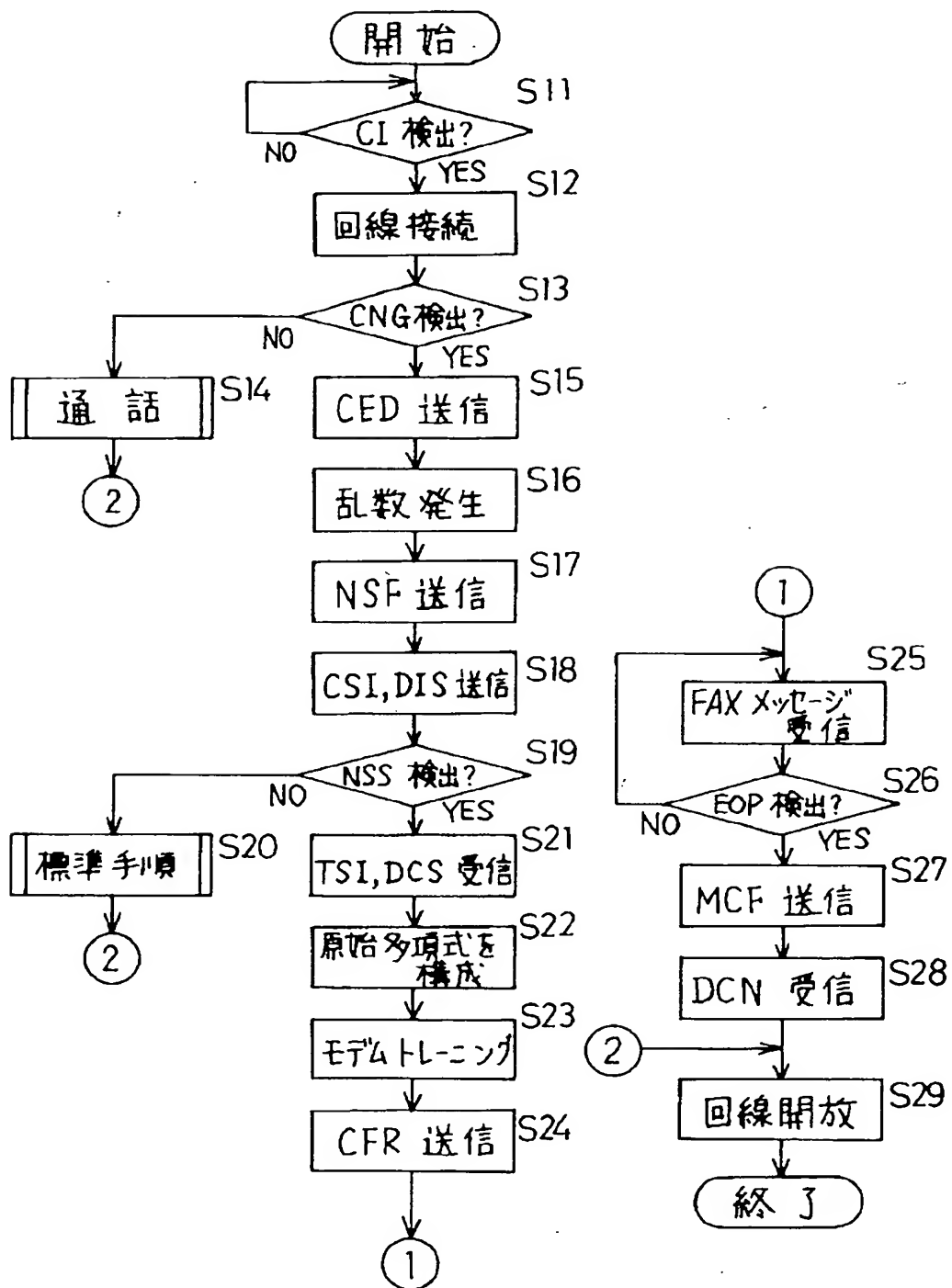
【図4】



【図5】



【図6】



【図 7】

